



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/484,691	01/18/2000	Hashem Mohammad Ebrahimi	1565.035US1	9980

21186 7590 07/22/2010
SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER

COLIN, CARL G

ART UNIT	PAPER NUMBER
----------	--------------

2433

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

07/22/2010

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@slwip.com
request@slwip.com

DETAILED ACTION

Response to Arguments

1. In communications filed on 4/26/2010, applicant amends claims 1 and 14. The following claims 1-22 are presented for examination.
2. Applicant's arguments, pages 7-9, filed on 4/26/2010, with respect to the rejection of claims 1-22 have been fully considered, but they are moot in view of a new ground of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-3, 7-17, and 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,401,125 to **Makarios et al** in view of US Patent 6,003,084 to **Green et al** in view of US Patent 6,985,953 to **Sandhu et al**.

As per claim 1, Makarios et al substantially teaches a method for brokering state information exchanged between computers using at least one protocol above a transport layer, the method comprising the steps of *receiving at a proxy a request from a client requesting a resource of an origin server wherein the transparent proxy is unknown to the client* (column 4, lines 53-56) the proxy disclosed meets the recitation of transparent proxy as the proxy is unknown to the client as the client sends the URL directly to a server. **Makarios et al** discloses *redirecting the client request from the proxy to a policy module* (a signup web page with an address) that meets the recitation of policy module with identifier of claim 14 (column 4, lines 51-53 and column 5, lines 10-15); obtaining enforcement data provided by the policy module (column 5, lines 15-27 and column 3, lines 1-10); a proxy cookie is generated in response to login information of the user and transmitting to the user to use as an authentication for further interactions with the proxy that meets the recitation of *generating at the transparent proxy a policy state token in response to the policy enforcement data* (column 5, lines 19-51); and *transmitting the policy state token from the proxy to the client wherein the policy state token is used as an authentication of the client to the transparent proxy for subsequent interactions between the client and the transparent proxy* (see column 5, lines 19-23). **Makarios et al** discloses *and the policy state token is represented as a transparent proxy cookie that maintains a relationship among the client, transparent proxy, and the origin server* (see column 5, lines 14-23); *the transparent proxy cookie includes an indication to the transparent proxy that the client has been authorized by the policy module to use the transparent proxy to access the resource of the origin server* (see column 5, lines 14-35). Although **Makarios et al** discloses the claimed

Art Unit: 2433

method steps of claim 1, **Makarios et al** does not provide enough details on the architecture implemented in the invention. **Green et al** in an analogous art teaches a memory configured at least in part by a transparent proxy process, a processor for running the transparent proxy process, (see figure 1) at least one link for networked communication between the transparent proxy process, on the one hand, and a client computer and an origin server, on the other hand, for example (see figures 2 and 3); **Green et al** further teaches a secure *transparent proxy is unknown to the client*, the transparent proxy is transparent to both a client and a server (column 9, lines 5-12) and transmitting packets in accordance with a defined security policy (column 5, lines 25-30) having a security module to verify whether to grant or deny access to proxy services (column 7, line 48 through column 8, line 25 and column 9, line 12-67). **Green et al** discloses a transparent proxy comprising a connection manager and a security manager that meets the recitation of *policy module residing within the same environment with the transparent proxy* (see figure 3b and column 5, lines 34-40). In one embodiment, the proxy comprises a connection manager and a security manager that meets the recitation of *policy module residing within the same environment with the transparent proxy* (see figure 3b and column 5, lines 34-40), the proxy incorporates features of both application gateways and proxies to better serve client or the server depending on which side caused the firewall action to be triggered; and further discloses several advantages of the invention associated with the transparent proxy (column 5, lines 55 through column 6, line 20). **Green et al** discloses wherein policy enforcement data is received from the policy module because as the client transfers data request to the proxy, requesting information from a server, the proxy comprises modules and components wherein a connection manager operates with a security monitor which monitors the data from the client for conformance with

predefined conditions and provides control information to the connection manager of the proxy which in turns controls the relay and directs it whether to establish connections to the server (see column 8, lines 14-25). In another embodiment, the proxy uses a filter component that also meets the recitation of policy module, and the filter component processes the policy enforcement data and returns status to the communication component of the proxy, based on the status, the proxy communicates accordingly to the server (see column 10, lines 28-47). Therefore, it would have been obvious to one of ordinary skilled in the art at the time the invention was made to modify the invention of **Makarios et al** to implement some of the features of the inventive concept of **Green et al**, which provides a transparent proxy comprising security modules with more security and more versatility as taught by **Green et al**. One skilled in the art would have been motivated to do so because the transparent proxy disclosed by **Green et al** is transparent to both the client and the server, incorporating features of both application gateways and proxies, easy to configure, (see column 5, line 55 through column 6, line 20), it also provides more security and more versatility where additional filtering may be performed as desired, and it is associated with policy module that allows the proxy to use any defined protocols in accordance to defined security policy and provides transparency wherein no devices need to change any configuration information (column 9, lines 11-60).

Makarios et al does not explicitly disclose *the indication represented as a key whose checksum is verified by the transparent proxy*. **Sandhu et al** in an analogous art discloses the transparent proxy cookie includes an indication to the transparent proxy that the client has been authorized by a policy module to use the transparent proxy to access the resource of the origin server, (see column 7, lines 21-22 disclosing using a proxy server to reach the Bob (the origin

Art Unit: 2433

server)); **Sandhu et al** further discloses the indication represented as a key whose checksum is verified by the transparent proxy (see column 9, line 40 through column 10, line 27; column 10, line 60 through column 11, line 7 disclosing verification server verifying the indication in the cookie represented as a key whose checksum is verified). Therefore, it would have been obvious to one of ordinary skilled in the art at the time the invention was made to modify the invention of **Makarios et al** to include an indication in the cookie, *the indication represented as a key whose checksum is verified by the transparent proxy* as taught by **Sandhu et al** because it would provide integrity to cookies ensuring a more secure transaction.

As per claim 14-17, Makarios et al substantially teaches a transparent proxy server comprising: *memory configured at least in part by a transparent proxy process, a processor for running the transparent proxy process, (see figure 1 and column 4, lines 29-34) at least one link for networked communication between the transparent proxy process, on the one hand, and a client computer and an origin server, on the other hand (see fig.1)*

wherein the client computer directs a request for a resource to an origin server and the request is intercepted by the transparent proxy process which is unknown to the client (column 4, lines 53-56) the proxy disclosed meets the recitation of transparent proxy as the proxy is unknown to the client as the client sends the URL directly to a server. Makarios et al discloses redirecting the client request from the proxy to a policy module (a signup web page with an address) that meets the recitation of policy module with identifier which identifies a policy module that grants or denies authorization of proxy services to the client computer; Makarios et al discloses obtaining enforcement data provided by the policy module (column 5, lines 15-27

Art Unit: 2433

and column 3, lines 1-10); a proxy cookie is generated in response to login information of the user and transmitting to the user to use as an authentication for further interactions with the proxy in response to the policy enforcement data (column 5, lines 19-51) that meets the recitation of *by acquiring policy enforcement data and attempting to authenticate the client computer to the transparent proxy process in response to the policy enforcement data* (column 4, lines 51-53 and column 5, lines 10-15); and transmitting the policy state token from the proxy to the client wherein *the policy module authenticates the client computer to the transparent proxy process for subsequent interactions between the client and the transparent proxy process* (see column 5, lines 9-23). **Makarios et al** discloses *and the transparent proxy creates a transparent proxy cookie for the relationship among the client, transparent proxy, and the origin server and the transparent proxy managed the transparent proxy cookie on the client* (see column 5, lines 14-23, note that the system is a computer program running on the transparent proxy (col.4, ll. 30-33)) ; *the transparent proxy cookie includes an indication to the transparent proxy that the client has been authorized by the policy module to use the transparent proxy to access the resource of the origin server* (see column 5, lines 14-35).

Although **Makarios et al** discloses the claimed server of claim 14, **Makarios et al** does not provide enough details on the architecture implemented in the invention. **Green et al** in an analogous art teaches *a memory configured at least in part by a transparent proxy process, a processor for running the transparent proxy process, (see figure 1) at least one link for networked communication between the transparent proxy process, on the one hand, and a client computer and an origin server, on the other hand*, for example (see figures 2 and 3); **Green et al** further teaches *a secure transparent proxy is unknown to the client*, the transparent proxy is

Art Unit: 2433

transparent to both a client and a server (column 9, lines 5-12) and transmitting packets in accordance with a defined security policy (column 5, lines 25-30) having a security module to verify whether to grant or deny access to proxy services (column 7, line 48 through column 8, line 25 and column 9, line 12-67). **Green et al** discloses a transparent proxy comprising a connection manager and a security manager that meets the recitation of *policy module processes within a same environment as the transparent process* (see figure 3b and column 5, lines 34-40). In one embodiment, the proxy comprises a connection manager and a security manager that meets the recitation of *policy module residing within the same environment with the transparent proxy process* (see figure 3b and column 5, lines 34-40), the proxy incorporates features of both application gateways and proxies to better serve client or the server depending on which side caused the firewall action to be triggered; and further discloses several advantages of the invention associated with the transparent proxy (column 5, lines 55 through column 6, line 20). **Green et al** discloses *a policy module that grants or denies authorization of proxy services to the client computer by acquiring policy enforcement data* because as the client transfers data request to the proxy, requesting information from a server, the proxy comprises modules and components wherein a connection manager operates with a security monitor which monitors the data from the client for conformance with predefined conditions and provides control information to the connection manager of the proxy which in turns controls the relay and directs it whether to establish connections to the server (see column 8, lines 14-25). In another embodiment, the proxy uses a filter component that also meets the recitation of policy module, and the filter component processes the policy enforcement data and returns status to the communication component of the proxy, based on the status, the proxy communicates

Art Unit: 2433

accordingly to the server (see column 10, lines 28-47). Therefore, it would have been obvious to one of ordinary skilled in the art at the time the invention was made to modify the invention of **Makarios et al** to implement some of the features of the inventive concept of **Green et al**, which provides a transparent proxy comprising security modules with more security and more versatility as taught by **Green et al**. One skilled in the art would have been motivated to do so because the transparent proxy disclosed by **Green et al** is transparent to both the client and the server, incorporating features of both application gateways and proxies, easy to configure, (see column 5, line 55 through column 6, line 20), it also provides more security and more versatility where additional filtering may be performed as desired, and it is associated with policy module that allows the proxy to use any defined protocols in accordance to defined security policy and provides transparency wherein no devices need to change any configuration information (column 9, lines 11-60).

Makarios et al does not explicitly disclose *the indication represented as a key whose checksum is verified by the transparent proxy*. **Sandhu et al** in an analogous art discloses the transparent proxy cookie includes an indication to the transparent proxy that the client has been authorized by a policy module to use the transparent proxy to access the resource of the origin server, (see column 7, lines 21-22 disclosing using a proxy server to reach the Bob (the origin server));

Sandhu et al further discloses the indication represented as a key whose checksum is verified by the transparent proxy (see column 9, line 40 through column 10, line 27; column 10, line 60 through column 11, line 7 disclosing verification server verifying the indication in the cookie represented as a key whose checksum is verified). Therefore, it would have been obvious to one of ordinary skilled in the art at the time the invention was made to modify the invention of

Makarios et al to include an indication in the cookie, *the indication represented as a key whose checksum is verified by the transparent proxy* as taught by **Sandhu et al** because it would provide integrity to cookies ensuring a more secure transaction.

As per claims 2-3, Makarios et al discloses the limitation of receiving at the proxy a renewed request for the origin server resource, the renewed request containing the policy state token, wherein the renewed request contains the policy state token in the transparent proxy cookie in a header sent from the client to the proxy, for example (column 5, lines 25-32).

As per claims 7-8, Makarios et al teaches the limitation of wherein HTTP or HTTPS is a protocol used during at least one of the receiving and transmitting steps (column 3, lines 30-67).

As per claim 10, the combination of **Makarios et al** and **Green et al** teaches directory access protocol for authentication of client that meets the recitation of utilizing LDAP as a software to provide authentication information about the client and the transparent policy enforcement data obtained by the transparent proxy depends on the authentication thus provided (**Green et al**, column 9, lines 12-47). Therefore, claim 10 is rejected on the same rationale as the rejection of claim 1.

Claims 9 and 11 are similar to the rejected **claim 10** except for utilizing Novell Directory Services and SSL software respectively instead of LDAP. **Green et al** discloses other

Art Unit: 2433

directory service protocols and any protocols used in X400's X500's. Therefore using NDS or SSL would have been obvious to one skilled in the art, as these protocols are well known.

Therefore, claims 9 and 11 are rejected on the same rationale as the rejection of claim 1.

As per claim 12, Makarios et al. teaches the limitation of wherein the obtaining step extracts policy enforcement data from a redirection address field (see column 3, lines 1-10).

As per claim 13, Makarios et al. teaches the limitation of wherein the transmitting step transmits the policy state token in the transparent proxy cookie in a header sent from the proxy to the client (column 10-32).

As per claims 20-22, claim 20 adds another proxy with similar limitations as the rejected claim 14. To one with ordinary skilled in the art, the network can comprise of any number of clients and servers and adding more than one proxy to share some of the functions would have been a design choice and obvious to one skilled in the art because assigning proxies to handle specific functions or protocols is well known in the art.

4. **Claims 4, 6, 18, and 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,401,125 to **Makarios et al** in view of US Patent 6,003,084 to **Green et al** in view of US Patent 6,985,953 to **Sandhu et al** as applied to claims 1-3 above and further in view of US Patent Publication US 2002/0007317 to **Callaghan et al**.

As per claim 4, **Makarios et al** discloses stripping in the proxy cookie to customize the client's information request as appropriate to the server (column 3, lines 1-10). **Callaghan et al.** in an analogous art teaches the step of forwarding to the origin server a portion of the renewed request, the forwarded portion omitting the policy state token (see page 6, paragraphs 88-90). **Callaghan et al.** further teaches in other embodiments the step of stripping off the state token (see page 4, paragraph 61 and page 5, paragraph 81). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to omit the policy state token when forwarding the request to server. One skilled in the art would have been motivated to do so because by omitting the policy state token the proxy can maintain the proxy cookie information secret to the server. The other advantage of adding and omitting state information as disclosed by **Callaghan et al** is that it enables a proxy to customize request and response as it fits to the proxy (page 4, paragraphs 61-62).

As per claim 6, **Callaghan et al.** teaches further comprising the steps at the proxy of forwarding to the client at least a portion of a communication from the origin server, and forwarding to the origin server at least a portion of a communication from the client (page 5, paragraphs 81-82). Therefore, claim 6 is rejected on the same rationale as the rejection of claim 4.

Claim 18 recites some of the limitations of claims 1 and 4 as discussed above. For instance, **Green et al** discloses transparent proxy service that is transparent to both client and server, the combined references above also teach the step of accepting the authorization from the

client with a renewed client request for the origin server resource; forwarding the renewed client request to the origin server without forwarding the authorization but with an indication to the origin server that the transparent proxy server is the source of the forwarded request, and then transparently forwarding the requested resource from the origin server to the client as mentioned in claims 1 and 4. Therefore claim 18 is rejected on the same rationale as the rejection of claims 1 and 4.

As per claim 19, Makarios et al teaches the limitation of wherein the transparent proxy server sends the client the authorization by sending the client a proxy cookie for use in subsequent communications from the client, for example (see column 5, lines 19-51).

5. **Claim 5** is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,401,125 to **Makarios et al** in view of US Patent 6,003,084 to **Green et al**, in view of US Patent 6,985,953 to **Sandhu et al**, in view of US Patent Publication US 2002/0007317 to **Callaghan et al** as applied to claim 4 above and further in view of US Patent 5,805,803 to **Birrell et al**.

As per claim 5, Makarios et al discloses an example of reply containing an origin state token for use by the proxy in its subsequent communications with a (column 5, lines 55-65). It is obvious to one skilled to the art that the same concept can be applied in the server side (see figure 2) as the proxy is capable of saving the cookie for future interactions with the server. **Green et al** discloses transparency with both the server and the client and discloses interaction

between the proxy and the server (column 11, lines 5-17). **Birrell et al.** in an analogous art discloses receiving at the proxy a reply from the origin server, the reply containing an origin state token for use by the proxy in its subsequent communications with the origin server, for example (see column 4, lines 51-65). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to include the step of receiving at the proxy a reply from the origin server, the reply containing an origin state token for use by the proxy in its subsequent communications with the origin server. One skilled in the art would have been motivated to do so because using the origin state token for use by the proxy in its subsequent communications with the origin server will allow the proxy to save in time and bandwidth if the server is already known to the server rather than authenticating at every session (column 4, lines 51-65 and 13-26).

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CARL COLIN whose telephone number is (571)272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kieu-Oanh (Krista) Bui can be reached on 571-272-7291. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Carl Colin/

Primary Examiner, Art Unit 2433

July 18, 2010